PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, H04L 29/06

A1

(11) International Publication Number: WO 98/44402

(43) International Publication Date: 8 October 1998 (08.10.98)

(21) International Application Number: PCT/GB98/00808

(22) International Filing Date: 18 March 1998 (18.03.98)

(30) Priority Data:
97302194.2 27 March 1997 (27.03.97) EP
(34) Countries for which the regional or international application was filed: GB et al.

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(71) Applicant *(for all designated States except US)*: BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY [GB/GB]; 81 Newgate Street, London EC1A 7AJ (GB).

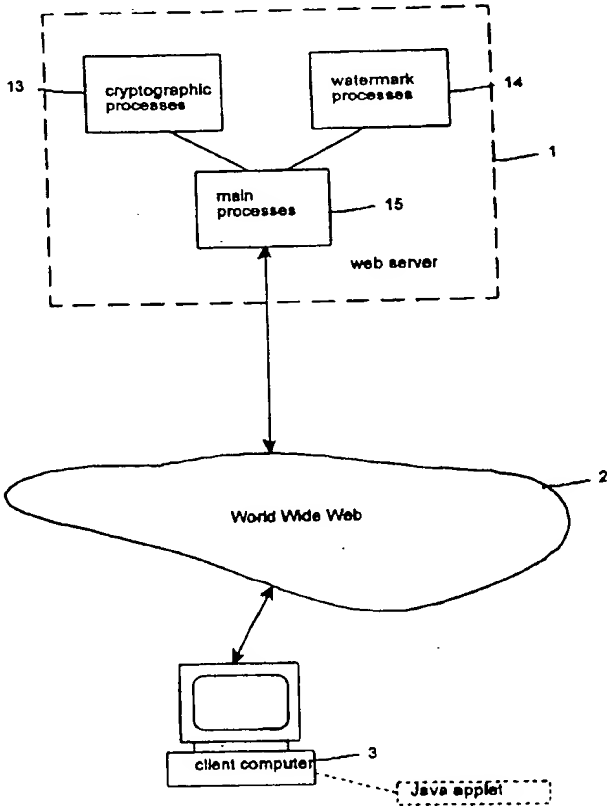
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: BRAMHILL, Ian, Duncan [GB/GB]; 76 Goring Road, Ipswich, Suffolk IP4 5LP (GB). SIMS, Matthew, Robert, Charles [GB/GB]; 39 Lister Road, Ipswich, Suffolk IP1 5EQ (GB).

(74) Agents: READ, Matthew, Charles et al.; Venner, Shipley & Co., 20 Little Britain, London EC1A 7DH (GB).

(54) Title: COPY PROTECTION OF DATA

(57) Abstract

A copyright protection scheme is provided in which data is downloaded from a server (1), typically over the World Wide Web (2) to a client (3), for presentation to a user. The downloaded data is cryptographically protected, by encryption and hashing. When displayed by the client, storing and copying functions are selectively disabled in respect of the data, in order to prevent unauthorised copying.



AL

Copy Protection of Data

Field of the invention

This invention relates to protecting data against copying and has particular application to protecting data transmitted through a network, such as hypermedia transmitted over a web-based network.

Background

It is known that data in the form of hypermedia such as hypertext, is often written in the hypertext language HTML and arranged in webpages that are provided by a server connected through a network to a client. The client may comprise a personal computer or other processing device capable of presenting the data retrieved from the server to a user. The network may comprise a local area network (LAN), a wide area network (WAN) or may comprise the Internet. For example, the World Wide Web comprises many servers connected over the Internet in a web, which have addresses in the form of universal resource locators (URL).

The hypertext information is arranged in webpages which include hotspots to allow the user to establish a link to another webpage, which may be located on the same or a different server, the routing to the document being achieved by use of a URL in the webpage at the hotspot.

Web clients typically access the hypermedia information using a browser. An overview of the World Wide Web and HTML is given in Chapter 1 of "HTML 3.2 and CGI Unleashed" J. December and M. Ginsberg 1996 (ISBN 1-57521-177-7).

As well known in the art, HTML webpages can display text, graphics and files of other descriptions such as video images, animated graphics and audio samples. Hypermedia have the significant advantage that the client can rapidly transfer viewing from one document to another by using a mouse to data over a network such as the World Wide Web, but is also applicable to LANs, WANs and to distribution of data using long term storage media such as 3.5" floppy discs or CD-ROM based technology.

The method of the invention may be used with a conventional browser.

A message concerning a webpage may be downloaded from the server to the client, the message including information concerning the program object, such that a request is then uploaded to the server in response to the message, in order to retrieve the program object. The webpage may be written in HTML code. The program object may comprise a Java applet although the invention envisages the use of other program objects such as Active X or OLE.

As a result of processing a Java applet, the usual copy and save functions will not be presented to the user, thereby providing security in respect of the unprotected data presented to the user.

The data presented may comprise text, graphics, pictures, audio or any other suitable form.

The program object may include data concerning a cryptographic key, which can then be used to render the downloaded cryptographically protected data into an unprotected form suitable for presentation to the user.

An authentication procedure may be employed to ensure that the cryptographically protected data is only downloaded to an authenticated client. The authentication process may be performed by reference to a payment scheme, to enable a royalty to be collected in respect of the downloaded, cryptographically protected data.

It will be understood that no copy protection scheme can ever be completely successful, because when data is presented to users, they will have the said unique determinator, and signalling to the server on the basis of the outcome of the comparison.

The client may be authenicated by the server prior to downloading the encrypted data.This may be carried out by generating a challenge, generating a response as a predetermined cryptographic function of the cryptographic key for the client as held by the server, and as a function of the key included in the unique determinator.stored in the client, and authenticating the client on the basis of the outcome of the comparison.

Brief description of the drawings

In order that the invention may be more fully understood an example will now be described with reference to the accompanying drawings, in which:

Figure 1 is a schematic illustration of a conventional client and server connected through the World Wide Web;

Figure 2 is a schematic illustration of a conventional display provided by a web browser on the client 3;

Figure 3 is a schematic illustration of a web server 1 connected to a client 3 through the World Wide Web 2, in accordance with the invention;

Figure 4 is a schematic illustration of the display of a web browser in accordance with the invention;

Figure 5 is a schematic illustration of data flows between the client and server in accordance with an example of the invention;

Figure 6 is a schematic flow diagram associated with step S10 of Figure 5;

Figure 7 is a schematic illustration of the BT copyright (BTC) file structure;

Figure 8 is a flow chart showing in detail the actions carried out during the wrapping step 10.5 of Figure 6;

Figure 9 is a schematic flow diagram associated with step S12 of Figure 5;

Figure 10 is a schematic illustration of data flows associated with a procedure for registering a client with the server; and

Figure 11 is a schematic illustration of authentication, subsequent to be produced of the entire page shown within the browser window 4. Also, the browser includes a control, shown schematically at 6, with a drop-down menu option "view source", which allows a display to be provided of the actual HTML code which is being run.

A page 7 is shown within the window 4 of the browser. The page is defined by a sequence of lines of HTML code which specify the text and layout provided on the page. Also, the code specifies areas which receive graphical, image data or other data that is downloaded in separate files which have a predetermined tag. In this example a graphics file with a tag "gif" is displayed. The HTML code causes the gif file to be displayed within the pre-defined area of the page. Thus, in the page 7, the gif file is displayed in region 8 defined by the downloaded HTML code. An example of the code for the gif file is shown in Code Extract No. 1, below.

Code Extract No. 1

```
CE1.1  <HTML>
CE1.2
CE1.3  <HEAD><TITLE>Company X's Homepage</TITLE></HEAD>
CE1.4
CE1.5  <BODY>
CE1.6  Welcome to Company X's Homepage
CE1.7
CE1.8  <IMG ALIGN=middle SRC="a_graphic.gif"><P>
CE1.9
CE1.10        <A HREF="another.html">link to another web page</A>
CE1.11        </BODY>
CE1.12
CE1.13        </HTML>
```

If the user clicks the computer's mouse in the area of the displayed image 8, using the right mouse button, a drop-down menu 9 is displayed which gives the user options including "save", to save the digital data corresponding to the gif file to the computer's hard disc or to some other storage location, and also the option to print, using a printer connected to the computer 3 (not shown). Thus, the user of computer 3 can make a copy of the digital data which comprises the graphics displayed in region 8 and the data can then be forwarded to other locations in an unrestricted manner. Because the data is although normally, gif files are downloaded directly into the webpage because it is not normally necessary to process them in terms of Java bytecodes.

The present invention provides a method by which data can be downloaded to the webpage in a secure manner, and cannot be saved or copied whilst being displayed without significant fraudulent effort.

An example of a downloading process in accordance with the invention will now be described in more detail with reference to Figures 3, 4 and 5. In this example, a webpage containing copyright protected image data is downloaded from the server 1 to client computer 3 through the World Wide Web 2. The resulting display in the browser 4 is shown in Figure 4 and the processing steps are shown in more detail in Figure 5.

At step S1 the client 3 uploads a request to the server 1 for details of a webpage. The request comprises a conventional hypertext file transfer protocol (HTTP) page request. The server then, at step S2, gets the page, or constructs it "on the fly" and downloads the HTML code corresponding to the page, to the client 3 through the World Wide Web (WWW) 2. In the usual way, the HTML code includes references for images, graphics, sound bytes and the like and in response to such codes, the server will upload HTTP requests for corresponding files to be displayed in the webpage. For example, referring to the webpage 7 shown in Figure 4, it includes a graphical image 11 constituted by a gif file. In order to obtain the data for the display 11, an HTTP request is uploaded at step S3 to the server, and corresponding binary graphical data is downloaded at step S4. This data is then displayed in region 11 of the page 7 shown in Figure 4. However, this data is not copyright protected because the user can save and copy it using the right mouse button as previously explained with reference to Figure 2.

However, in accordance with the invention, region 12 of the displayed page 7 is copyright protected. The HTML code associated with the page 7 of Figure

The applet A1 is run at step S7 on the client computer 3 and at step S8, the applet causes a BTC file request to be uploaded to the server 1.

At step S9, the server performs an authentication step in order to determine whether it is safe to download the requested BTC file to the client. The authentication may be carried out in a number of different ways. For example, the server may only download the file if the client has made a payment, so as to allow the owner of the copyright of the BTC file to collect a royalty for the act of viewing the file. A micropayment scheme for this purpose is described in our co-pending patent application No. GB 9624127.8 entitled Transaction System. Alternatively, the client 3 may be known to the server in respect of some other service being provided, for example an Internet home shopping scheme, and the client's credentials may be authenticated by means of procedures already in use for the service.

Assuming that the client 3 passes the authentication step S9, the server then, at step S10, prepares the BTC file for downloading to the client 3.

The step S10 is shown in more detail in Figure 6. At step S10.1 the relevant data is fetched. This may comprise graphics data, audio, video, text or an other appropriate data format.

At step S10.2, the data is watermarked. This may involve changing some of the bits in the data stream so as to record a pattern which is imperceptible in the image displayed by the browser 4, when the data is downloaded to the client. Watermarking is a well known example of a technique termed steganography. For a general review of this technique and digital watermarks, reference is directed to "Disappearing Cryptography", P. Wayner, Academic Press 1996 (ISBN 0-12-738671-8). Watermarking gives additional security in the event the protected data is copied, because knowledge of the source of copying can be determined from the watermark. Thus, if the authentication step (step S9) provides the server with a particular identity for

The BTC file in step S10.5 is generated as follows. In step S10.5.1 partial information for the header H is generated. This comprises a version number for the file format, and any specific copyright protection control information CI for the file.

In step S10.5.2 the integrity of all of this information is protected by generating a hash value HV_{head} using a hashing key HK_{head}.

In step S10.5.3 the hashing key used on the header HK_{head}, and the generated hash value HV_{head} are both appended to the header H, so as to complete it.

In step S10.5.4 the watermarked, and encrypted file generated in step S10.4 is appended to the header H to form part of the embedded file EF in Figure 7.

In step S10.5.5 information which describes the hashing that was performed in step S10.3 is appended to the file EF. This information comprises the specific session hashing key K_{SH} used on the embedded file hereinafter referred to as $HK_{embedded}$ and the hash value HV generated in step S10.3 hereinafter referred to as $HV_{embedded}$. This completes the BTC file.

At step S11 (Figure 5) the BTC file is downloaded to the client 3.

Then, at step S12, the BTC file is processed using the applet A1 previously downloaded to the client 3. The processing performed at step S12 is shown in more detail in Figure 9. At steps S12.1 and S12.2 the integrity of the content of the header H is verified. In step S12.1, using the hashing algorithm HA, and the hashing key used on the header HK_{head} (recovered from the header H of the BTC file) the hash value HV_{head} of the header is generated. At step S12.2 the value is checked against the hash value HV_{head} recovered from the BTC file header H.

If the result of the check is unsatisfactory, an error banner is displayed at step automatically provided for saving, copying or printing the displayed data in region 12. The right mouse button function is disabled according to usual Java operation for applets as previously described. The user could operate the print button 5 of the browser 4 but this would only print a low quality image and would not permit the digital data that comprises the image 12 to be recovered for the purpose of providing a high quality copy.

Furthermore, if the downloaded BTC file is cached in the browser, it will be cached in its cryptographically protected form so that making copies of the cached file does not permit access to the downloaded data in the BTC file, unless substantial code breaking activities are fraudulently undertaken by the user.

It will be understood that no copyright protection scheme can ever be completely successful because when a copyright work is presented to a user, they will have an opportunity to copy it. The purpose of the present scheme however, is to make payment of a small monetary sum in respect of the copyright protected work, more attractive than the effort of breaking the protection regime provided by the invention. An analogy can be drawn with copying pages of a book with a photocopier. In theory, it would be possible to borrow a book and then photocopy all of its pages. However, in practice, this is very inconvenient and it is probably easier to purchase another copy of the book. Similarly, in the described example of the invention, it is simpler to pay for viewing of the copyright work than spending time breaking the copyright protection scheme.

Many modifications and variations fall within the scope of the invention. For example, the running of the applet A1 may be modified according to the downloaded copyright control information CI in order to provide a restricted set of functions when operating the right mouse button on the display area 12. For example, operation of the right mouse button on the display area 12 may optionally provide a drop down menu which offers the user a copyright

At step R3, the dogtag program is run in order to provide a machine identification code (MID) which provides a substantially unique identification of the client. The dogtag program scans the client computer both in terms of its hardware and software. Examples of characteristics of the client which can be used to form the MID are as follows:

The physical components of which the computer comprises (size of memory, presence of CD drive)
Characteristics of the physical components (manufacturer, number of tracks on a hard disc)
Location of static information on a hard disc (bad sectors)
Location of long lived files on a hard disk (operating system executables)
Operation characteristics
Logical directory and file structures
Files specifically created to identify the machine
Data added to long lived files to identify the machine
The configuration of applications and the operating system
Identification number of hardware, e.g. hard disc.

For added security, the dogtag can only be run once for registration purposes.

At step R4, the MID is uploaded through the WWW 2 to the web server 1. At step R5 an individual cryptographic key K_1 is embedded together with the MID in the bytecodes of the Java applet which is then downloaded at step R6 to the client 3 and is stored on the hard disc thereof at step R7. The individual key K_1 actually comprises a set of keys, individually provided for each client 3 for use in hashing and encrypting as previously described.

Referring now to Figure 11, this shows how the authentication step, step S9 in Figure 5, can be performed, subsequent to the registration procedure of Figure 10.

provision of keys and watermarking can be performed as a separate service to a number of different web servers.

Whilst the described example of the invention uses the Java programming language, it will be understood that other hypermedia languages may be used, for example Active X and OLE.

The registration and authentication procedure described with reference to Figure 10 and 11 may also be used for other authentication processes in which a client is required to register with a web server. Thus, this procedure could be used for processes which involve other data transfer regimes between the client and server in which a registration and authentication is needed.

for presentation to the user,
the program object being operative such that no, or restricted, copy or save functions are offered to the user in respect of the downloaded data in its unprotected form.

8. A method according to claim 7 including downloading a message concerning a webpage wherein the message includes information concerning the program object, and uploading a request for the program object in response to said information in the message.

9. A method according to claim 8 wherein the message is in HTML code.

10. A method according to claim 8 or 9 wherein the program object comprises a Java, Active X or OLE applet.

11. A method according to any one of claims 7 to 10 wherein the message is presented to the user through a browser.

12. A method according to any preceding claim wherein the data is sent to the client from the server through a network.

13. A method according to claim 12 wherein the network comprises the World Wide Web.

14. A method according to any one of claims 7 to 10 wherein the program object includes data concerning a cryptographic key, and including using the key to render the downloaded cryptographically protected data into an unprotected form suitable for presentation to the user

15. A method according to any preceding claim wherein the server and the client each hold data corresponding to a cryptographic key and a machine identifier for uniquely identifying the client, the method including:

any preceding claim.

22. A method of downloading encrypted data from a server to a client, including:

registering the client with the server by

determining a machine identifier of the client by analysing its hardware and/or its software configuration,

transmitting the machine identifier to the server,

combining the transmitted machine identifier with a cryptographic key to form a unique determinator for the client, and

transmitting the unique determinator to the client, to be stored therein for use subsequently in identifying the client to the server, to permit encrypted data to be downloaded thereto from the server;

subsequently identifying the client to the server on the basis of the unique determinator; and then

downloading data encrypted by means of the cryptographic key to the identified client, for decryption by the client using the key from the unique determinator.

23. A method according to claim 22 including decrypting the downloaded data at the client using the key from the unique determinator.

24. A method according to claim 22 or 23 wherein the client is identified to the server by again determining the machine identifier for the client, comparing it with the machine identifier included in said unique determinator, and signalling to the server on the basis of the outcome of the comparison.

25. A method according to claim 22, 23 or 24 including authenticating the client to the server prior to downloading of the encrypted data.

26. A method according to claim 25 including generating a challenge, generating a response as a predetermined cryptographic function of the

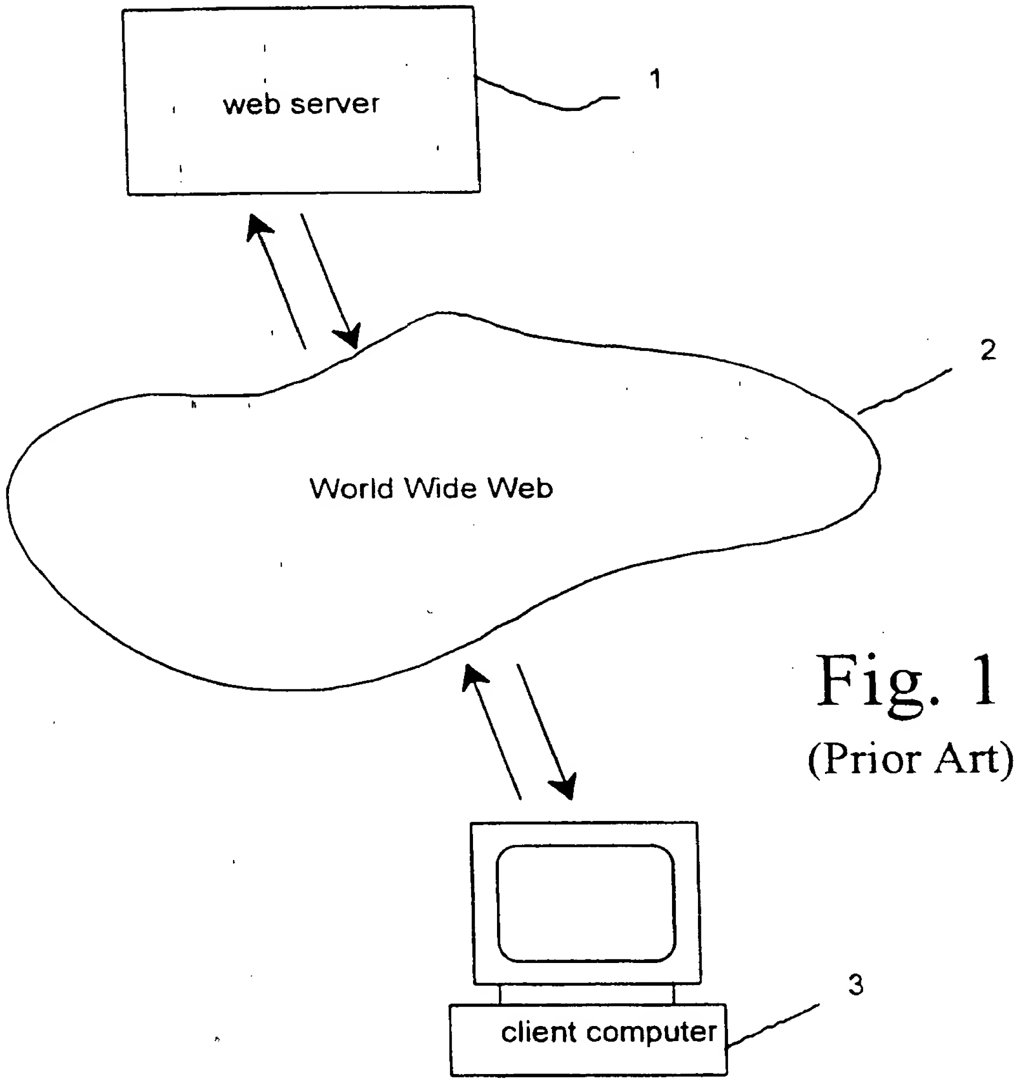


Fig. 1
(Prior Art)

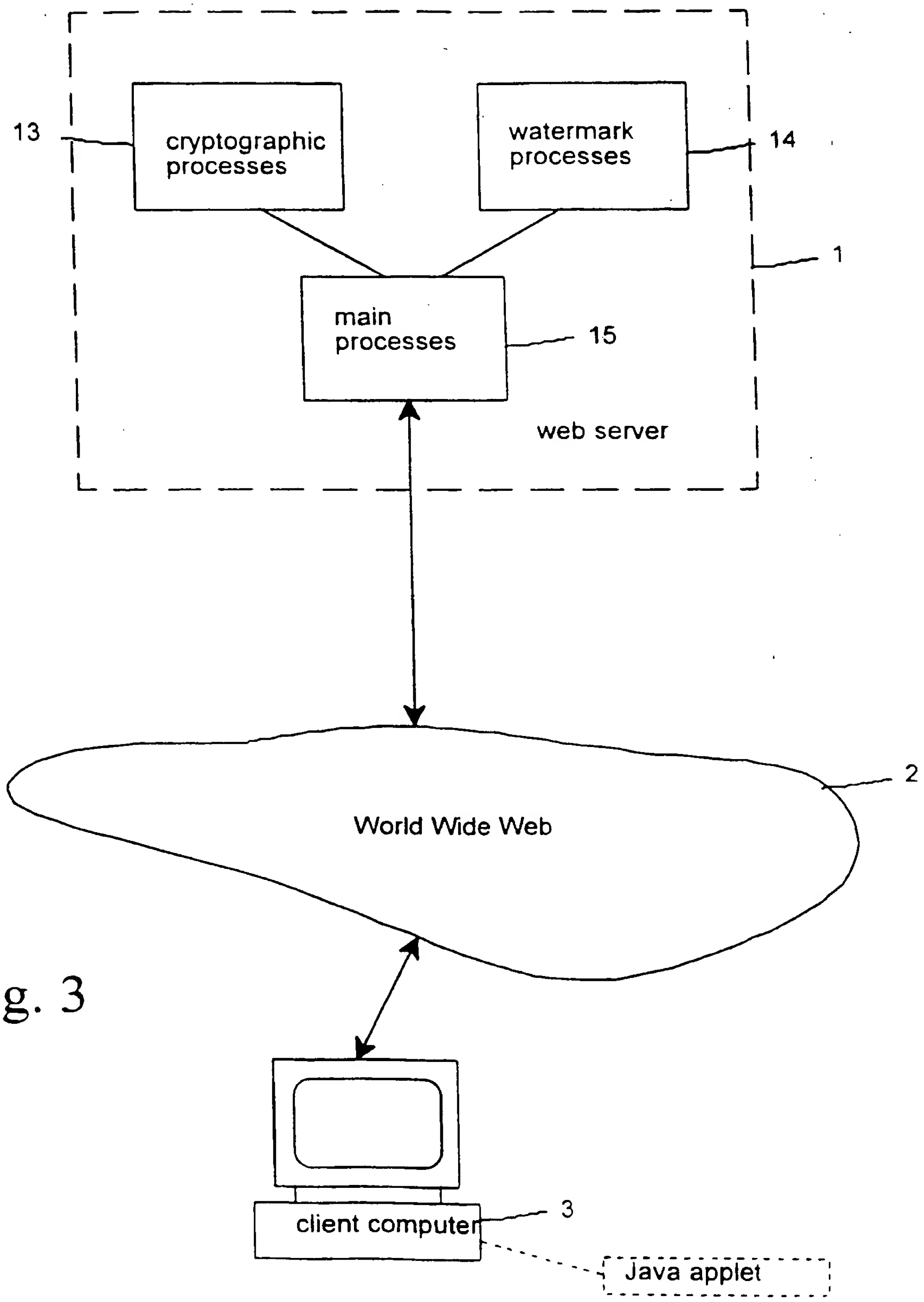

13
cryptographic processes
watermark processes
14
1
main processes
15
web server
World Wide Web
2
client computer
3
Java applet

Fig. 3

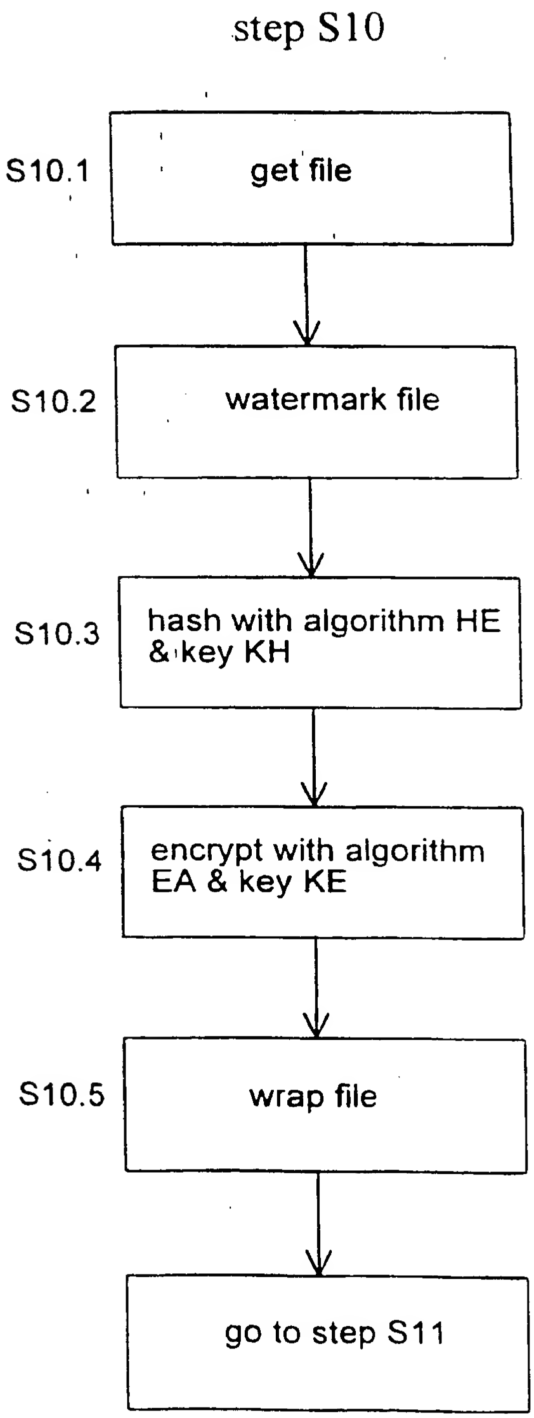
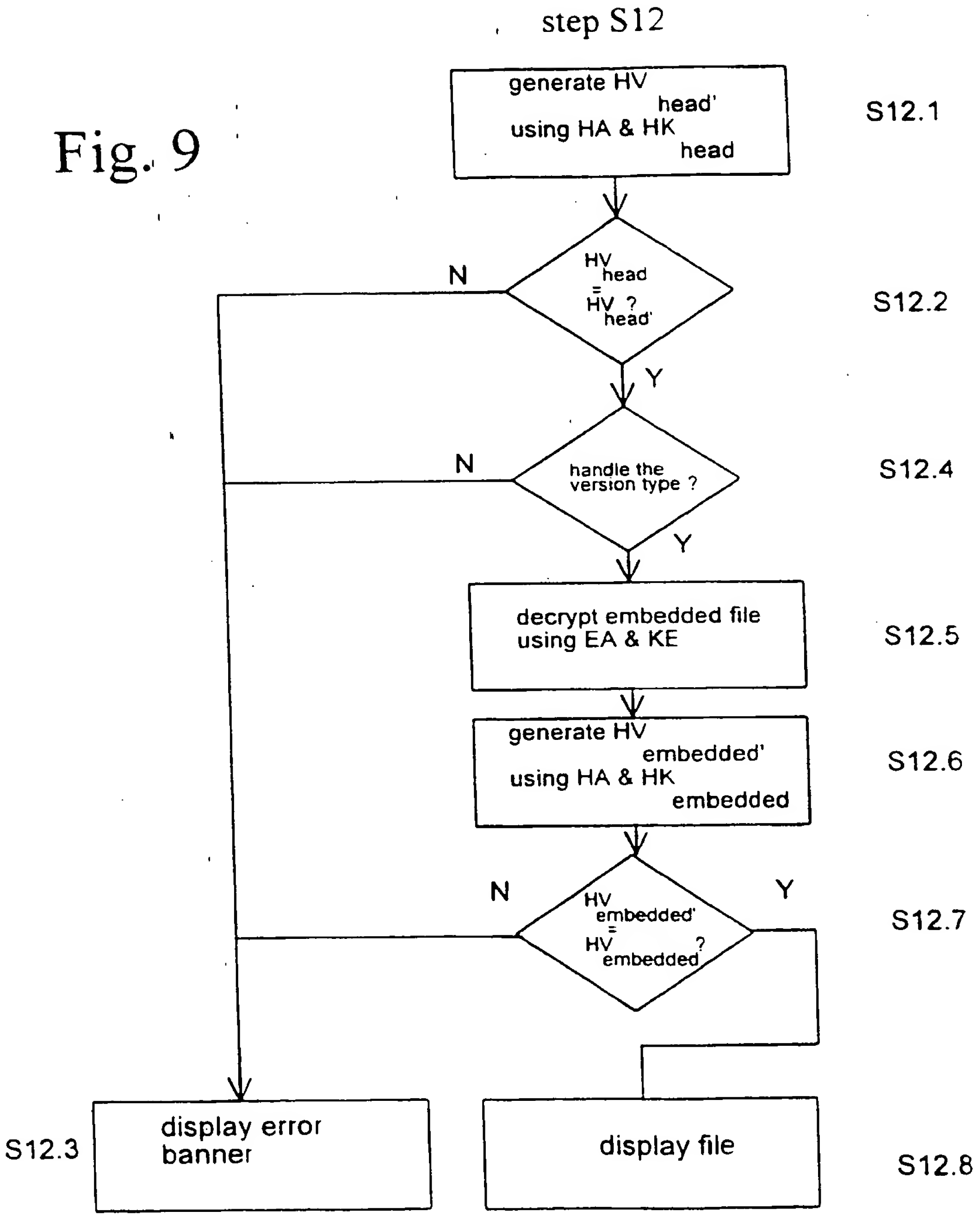

step S10
S10.1
get file
S10.2
watermark file
S10.3
hash with algorithm HE & key KH
S10.4
encrypt with algorithm EA & key KE
S10.5
wrap file
go to step S11

Fig. 6

Fig. 9


step S12
generate $HV_{head'}$ using HA & HK_{head}
S12.1
$HV_{head} = HV_{head'}$?
S12.2
N
Y
handle the version type ?
S12.4
N
Y
decrypt embedded file using EA & KE
S12.5
generate $HV_{embedded'}$ using HA & $HK_{embedded}$
S12.6
$HV_{embedded'} = HV_{embedded}$?
S12.7
N
Y
display error banner
S12.3
display file
S12.8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 98/00808

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 94 07204 A (UNILOC CORP PTY LIMITED ;UNILOC SINGAPORE PRIVATE LIMIT (SG); RICH) 31 March 1994 see abstract; figures 2,3,7-9 see claims 1-30	22,23, 25,27
A		15,17-19

Y	US 5 235 642 A (WOBBER EDWARD ET AL) 10 August 1993 see abstract; figure 2 see claims 1-9	22,23, 25,27

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 23 June 1998	Date of mailing of the international search report 01/07/1998
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Powell, D

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 98/00808

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9407204 A	31-03-1994	AU 678985 B	19-06-1997
		AU 4811393 A	12-04-1994
		CA 2145068 A	31-03-1994
		CN 1103186 A	31-05-1995
		EP 0689697 A	03-01-1996
		NZ 255971 A	26-05-1997
		US 5490216 A	06-02-1996
US 5235642 A	10-08-1993	EP 0580350 A	26-01-1994
		JP 6202998 A	22-07-1994
EP 0718761 A	26-06-1996	US 5630066 A	13-05-1997
		JP 8263447 A	11-10-1996